Methodology to Align Business and IT Policies: Use case from an IT Company

Feltus, Christophe; Incoul, Christophe; Aubert, Jocelyn; Gâteau, Benjamin; Adelsbach, André; Camy, Marc

Published in:
Proceedings of the ARES 2009 Workshop on Organizational Security Aspects (OSA), Fukuoka, Japan

DOI:
10.1109/ARES.2009.47

Publication date:
2009

Document Version
Early version, also known as pre-print

METHODOLOGY TO ALIGN BUSINESS AND IT POLICIES: USE CASE FROM AN IT COMPANY

Christophe Feltus[1], Christophe Incoul[1], Jocelyn Aubert[1], Benjamin Gateau[1], André Adelsbach[2], and Marc Camy[2]

[1]Public Research Centre Henri Tudor, Luxembourg
[2]Telindus PSF, Luxembourg

Abstract: Governance of IT is becoming more and more necessary in the current financial economic situation. One declination of that statement is the definition of corporate and IT policies. To improve that matter, the paper has for objective to propose a methodology for defining policies that are closer to the business processes, and based on the strict definition of a responsibility model that clarify all actor's responsibility. This responsibility model is mainly defined based on the three concepts of capability, the accountability and the commitment. The methodology is illustrated and validated based on a case study conducted in an IT company.

***Index Terms*— Governance, Process model, Organizational model, Responsibility model, Policy Engineering, Business IT Alignment.**

I. INTRODUCTION

Accounting scandals of 2002 and more recently ongoing market crisis highlight the importance of the Corporate Governance and by consequence: *Governance of IT*. Following those scandals, a lot of laws and standards were published in order on one hand to guarantee the stability of the financial sector and, by extension, to all sectors of the industrial economy and in the other hand, to enhance the governance all of these public and private companies. Sarbanes-Oxley Act [1], Basel II [2] and EU Directive 95/46 [3] are some of these laws that aim at providing guarantees over the company's accountability. The ISO/EIC 38500:2008 [4] is one standard that provides a framework for effective governance of IT. One of the main constraints imposed by these laws and standards is to have responsibilities clearly established and accepted internally by the collaborators and externally by the stakeholders as well. Unfortunately, by depicting the responsibility in a large range of IT oriented frameworks, we come to the conclusion that no global consensus over a responsibility model exists. The scope of our review as targeted organizational models from the realm of IT security, from access control models such as RBAC [7], UCON [8] and OrBAC [9], up to framework for ICT governance like Cobit and its RACI chart [10] or the service management like ITIL [11]. We have also investigated the area of requirement engineering, through the analyses of role engineering methods like [12], [13], [14] and [15] and through EAM (Enterprise Architecture Model) frameworks like CIMOSA [16] or Togaf [17]. The importance of the finding regarding the miss of a common understanding over responsibility has oriented our research and as a consequence, we propose in this paper firstly to introduce our innovative responsibility model that has been elaborated following the review and based on a global comprehension of the concepts. This model has already been largely commented in [5] and [6]. It has been designed to be a structured representation of the responsibility necessary to achieve a finite set of activities (like those encompassed in a process). The three main components of the responsibility model are Capability, Accountability and Commitment. The capability describes the quality of having the required qualities or resources to achieve a task, the accountability describes the state of being answerable about the achievement of a task, and the commitment is the engagement of a stakeholder to fulfil a task and the assurance he will do it. Hence, the usage of our model may not be dissociated from the usage of those other models and when we use them together, the organizational model is enhanced with responsibility concept and is as a consequence closer to governance requirements.

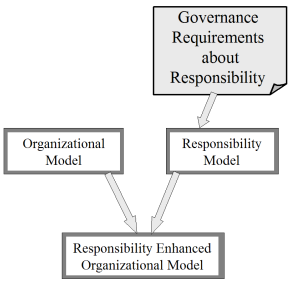

Fig. 1. Model aggregation

In Fig. 1, Governance requirements are those dictated by newly arising laws and standards like the need for more ethics, more commitment or more accountability. The engineering of these requirements has been performed in [5] and [6]. The responsibility model represents the model of responsibility that has been designed based on these requirements. The organizational model is the model to be enhanced with the responsibility components and could be for example the Cobit framework, the Cimosa framework or a process based enterprise architecture. That last case has already been investigated in previous work where a link has been created between ISO/IEC 15504 and the responsibility model [18].

Secondly the paper proposes a method to instantiate that responsibility model based on the enterprise description. This instantiated model is an intermediary model to be linked to the organizational model (like a workflow). This method is a five steps approach starting with a phase of information collection and closing with a corporate policy. It exists a plethora of definitions of policy. For the purpose of that paper, we use the following interpretation that a policy is a set of roles and responsibilities for a dedicated area of a

company or for a field of activity and consequently we decide to illustrate the paper for policy of access control.
The remainder of the paper is organized as follows: the next section introduces our innovative responsibility model, Section III introduces the five steps of our proposed methodology and illustrates it at the meantime by a real case study from an IT company. Finally, Section IV concludes and introduces future works.

II. Responsibility Model

The cornerstone of the methodology we propose in this article, and which we will detail in Section III, is based on the concept of responsibility. The model of responsibility in Fig. 2 aims to be generic enough to be applied to all kinds of organisations, at each abstraction layer and all domains of the organisation. In short, the organisation represents a structure that pursues collective goals. This structure encompasses employees (users) playing roles and that are responsible to perform processes' activities. In this model, the notion of sequence (the workflow) between the different responsibilities is not represented. Indeed, these transitions are already defined in the other organizational models defining the process model like ISO/IEC 15504.
The notion of responsibility is widely used, but no unique definition exists. According to the literature, we may however state that commonly accepted definitions of responsibility encompass the idea of having the obligation to ensure that something happens. Our previous work [5] shows that *responsibility* can be described as a set of three additional elements that are Capability, Accountability and Commitment. The relation between responsibility and the three other concepts is of the form 0.* to 1. That means that being responsible involves that the possibility to dispose of many Capacities, Accountabilities and Commitment.

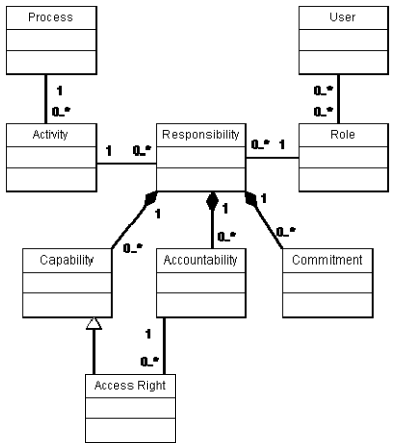

Fig. 2. Responsibility model

Capability describes the quality of having the required qualities or resources to achieve a task. For instance, a strategic capability for a given responsibility could be: "A resource must know the strategic objectives of the organisation". An operational capability could be: "The coach of the resources must have write access to the HR software".
Accountability describes the state of being accountable on the achievement of a task. For instance, a strategic accountability for a given responsibility could be: "A project leader must achieve the financial Key Performance Indicators defined for the project". An operational accountability could be: "An IT administrator must give access rights to specific resources of the organisation to members of the project team".
Finally, *Commitment* is the engagement of a stakeholder to fulfil a task and the assurance that he will do it. For instance, a strategic commitment for a responsibility could be:" The Chief Financial Officer accepts to manage the accounting department and not commit insider dealing". An operational commitment could be: "An employee of the procurement staff accepts not to use the system for his personal use".

The consistency between concepts may also be examined based upon the assumption that the capability needed for assuming a responsibility corresponds to the accountability of another responsibility (belonging to another user or role). Both responsibilities' components capability and accountability are strongly linked to each other [5]. An accountability of a role or a person can permit to deduce capability of another role or person and conversely a capability stems from accountability (e.g.: The capability "The coach of the resources must have write access to the HR software" stems from the accountability "An IT administrator must give access rights to specific resources (HR software) of the organization to the coach").

III. Methodology

The methodology described in this section has for objective to explain how to define the enterprise IT policies according to the responsibility model. This methodology is a five steps approach. To facilitate the understanding, we illustrate each step with a case study.

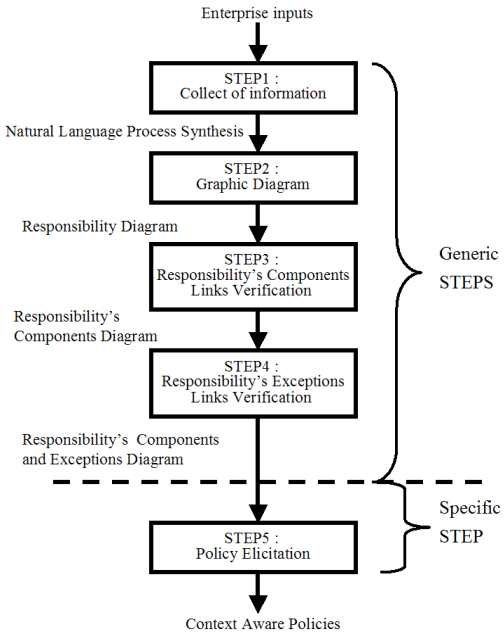

Fig. 3. SIM Methodology

3.1 STEP 1. Collect of information

The first step has for objective to define the context and to collect each component that will be formalized in the policy.

STEP 1 input: Inputs of step 1 are elements collected from business case studies, business processes, business procedures, and effective practices in the enterprise.

STEP 1 output: Output of step 1 is a formalized and structured synthesis of the process in natural language.

STEP 1 actions: The actions performed at this step encompass a number of activities to collect information about the process and the responsibility components. These activities are interviews of the key members of the personnel, analyses of existing process descriptions, analysis of enterprise referential like the ISO 9000 quality book.
By these activities, we can summarize by: process responsibilities as well as their composing elements, like accountabilities, capabilities, and commitments. The existing relations between responsibilities and responsibility components.
To illustrate that methodology, we describe this first step based on a case study. Telindus Luxembourg SA is an ICT company within the Belgacom Group, offering its services in the field of telecommunications and information systems. Telindus SA is ISO 9001 certified and, as such, formally defined several processes. For the case study the process of customer complaints will be analysed.
The customer complaints procedure in Fig. 4 defines the process of opening, the pursuing and the closing of customer complaints in order to resolve complaints with a short delay and, thereby, further improving customer satisfaction.
Complaints are registered in a central complaint database and assigned to an owner. A central complaint database is used to track complaints throughout their lifecycle and documenting actions that have been taken to resolve them, but also the lessons learned to prevent similar complaints or supporting their resolution more effectively in the future.

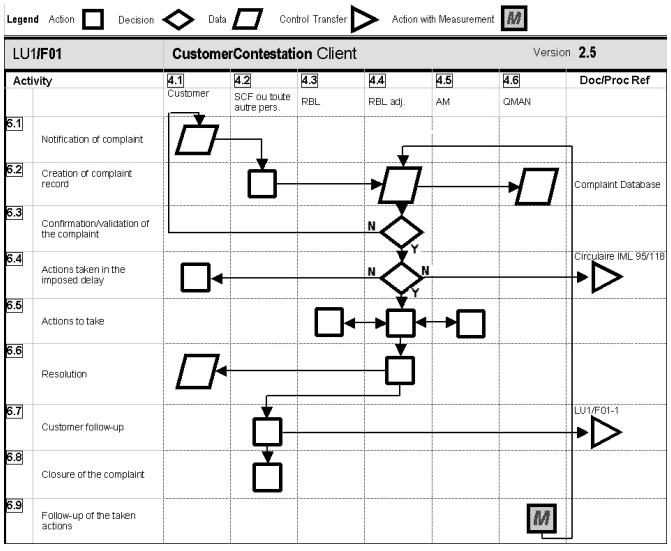

Fig. 4. Contestation Client process workflow

3.2 STEP 2 Graphic diagram

The second step translates the process from natural language into a graphical representation.

STEP 2 input: Input of Step 2 is the synthesis achieved in step 1.

STEP 2 output: Output of Step 2 is a graphical representation of the responsibility framework of the analysed process. It encompasses a representation of the responsibility and its components, and the links between components. The Fig.9 is an example of result obtained with the Telindus Case study.

STEP 2 actions: The actions performed at that step are composed of three sub-tasks.

Sub-task 1: Definition of each responsibility and transcription of it using boxes. Each box stands for a responsibility; it encompasses its accountabilities and its capabilities. An example identified within the case study is the responsibility "Creation of Complaint Report" in the contestation process.

Sub-task 2: For each responsibility, an analysis of the required capabilities is made and is translated through a box in the corresponding responsibility box. The same operation is performed for the accountabilities. The "Creation of Complaint Report" responsibility requires the capability to receive customer complaints and write access to the central complaint database. Accountabilities of this responsibility are, amongst others, to register the complaint in the database.

Sub-task 3: This last sub-task consists in the definition of links between responsibilities components. Four kinds of links exist:

- *Delegation link* constituting the delegation of a responsibility's accountability toward another responsibility. The responsibility of the achievement of the task is transferred to another responsibility, but the state of being answerable about the achievement of the task persists for the delegating responsibility.

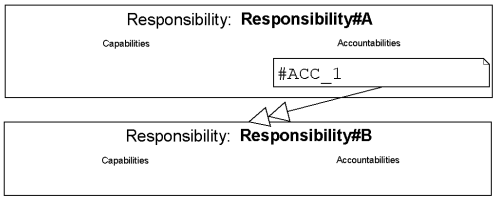

Fig. 5. Delegation link

For instance, Fig. 5. represents a delegation of the accountability #ACC_1 of the responsibility Responsibility#A towards the responsibility Responsibility#B. In the case study the accountability "validation of complaint" of the responsibility "Creation of Complaint Report" is delegated to the responsibility "Confirmation/Validation of Complaint".

- *Implication link* representing the connection between the accountability of one responsibility with the capability of another responsibility. It permits to formulate that this accountability is needed to provide and guarantee a capability to another responsibility.
It is important to note that an accountability of a responsibility may not aim at providing capability to the same responsibility. Conceptually, this situation would mean that this responsibility is divisible in two responsibilities.

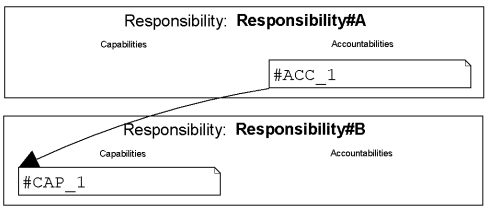

Fig. 6. Implication link

For instance, Fig. 6. illustrates that the accountability #ACC_1 of the responsibility Responsibility#A implies the capability #CAP_1 of the responsibility Responsibility#2. As an example consider the implication from accountability "Assure the first level of complaint closure" ("Resolution Acknowledgement" responsibility) to the capability "Acknowledgement of the complaint closure".

- *Contribution link* highlighting that one responsibility's accountability contributes to another accountability of the same responsibility. Accountabilities results can be used as input for others accountabilities.

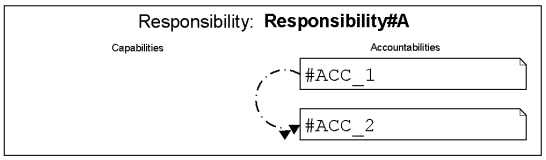

Fig. 7. Contribution link

For instance, Fig. 7. represents that the accountability #ACC_1 contributes to the accountability #ACC_2 of the same responsibility Responsibility#A. Considering the case study (Figure 9), we see that accountability "Register the complaint in the database" contributes to the accountability "Assign complaint to the RBL technical or commercial assistant", because the complaint can be assigned by the database when registering it.

- *Execution link* formalizing that a capability of a responsibility is necessary to execute an accountability of the same responsibility.

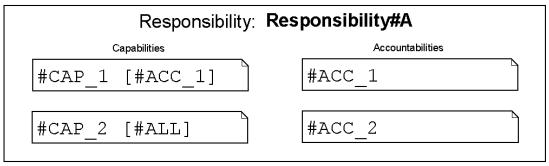

Fig. 8. Execution link

For instance, Fig. 8. illustrates that the capability #CAP_1 is needed to achieve the accountability #ACC_1 (written inside brackets in the capability CAP_1 definition). The capability #CAP_2 is needed for achieving both accountabilities #ACC_1 and #ACC_2 (because of the #ALL reference written inside brackets).. An example from the case study is that the capability "read access rights in the complaints database" is needed to "Verify the evolution of the complaint until closure" (responsibility "Follow-up of the taken actions")

3.3 STEP 3 Responsibility's components links verification

This third step of the methodology is the first refining step. It aims at analysing the graphical representation of the process issued from Step 2, depicting and eliminating inconsistencies from the diagram.

STEP 3 input: Input of Step 3 is the process graphical representation issued from Step 2.

STEP 3 output: Output of Step 3 is a graphical representation of the responsibility framework of the analysed process refined according to the components relationships.

STEP 3 actions: The actions performed at that step are composed of three sub-tasks.

Sub-task 1: Deep analysis of the capability components for each responsibility. The main objectives of this analysis are to detect and solve the problem of unnecessary capabilities. Capabilities may be unnecessary in the case of useless capabilities for the achievement of accountabilities of the same responsibility. This means that they do not have execution links. To face this inconsistency, it is necessary to suppress the capability.

Sub-task 2: Deep analysis of the accountability components for each responsibility. The main objective of this analysis is to make sure of that all accountabilities are provided and exist in the model, and to assure that all accountabilities are necessary. Some accountabilities are not fully justified if:

a. No link exist between the accountability with one or more capabilities in the process. That means that there's no implication link starting from the accountability
b. No link exist between the accountability and another responsibility. That means that there's no delegation link starting from this accountability
c. The accountability does not contribute to achieve the outcome of the process.

Sub-task 3: Once accountabilities are verified, it is possible to check that all capabilities necessary for their achievement exist.

3.4 STEP 4 Responsibility's exceptions links verification

This fourth step of the methodology is the second refining step. As step 3, it aims at analysing the graphical representation of the relation within the process, in order to depict inconsistencies and correct the graph to eliminate them if necessary.

STEP 4 input: Input of Step 4 is the process graphical representation issued from Step 3.

STEP 4 output: Output of Step 4 is a graphical representation of the responsibility framework of the analysed process refined according the relationship between components.

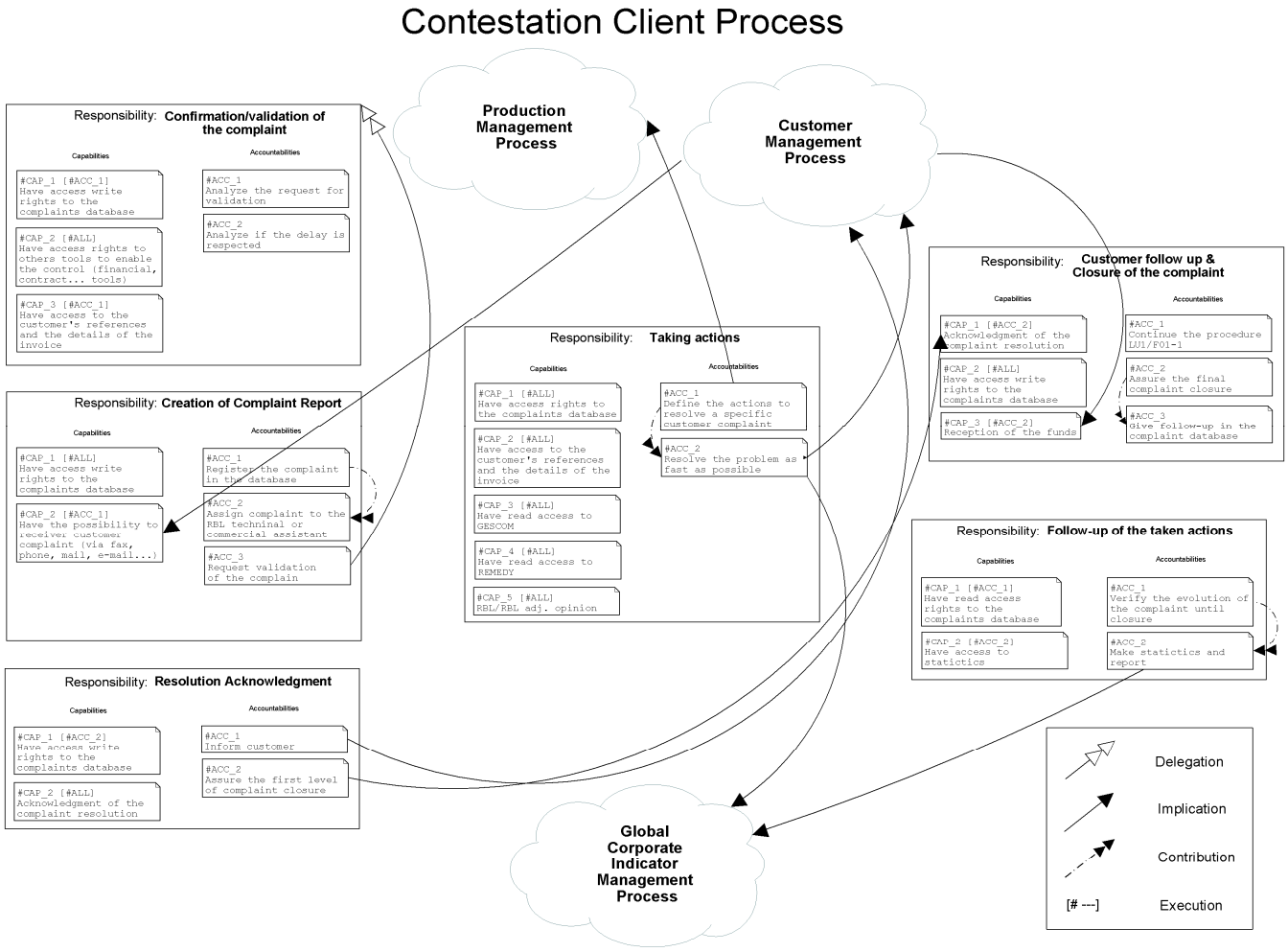

Fig. 9. Contestation Client Process responsibility model

STEP 4 actions: The activity of that step aims at detecting and correcting conflicts and incoherencies with regard to responsibility rules dictated by the enterprises, for example:

- *Delegation rules*. The organisation should define rules for delegation, which must be complied. Example of that delegation rules are: if a responsibility is delegated, all the capabilities necessary for it are also delegated and the accountability may be kept by the delegator or given to the delegate but not both at the same time. Some conflict may exist regarding that rule.

- *Separation of duties*. Some corporate rules may impose the separation of duties for some responsibility components. At this step, a check has to be done, in order to detect responsibility components that can potentially confer too much power, in order to prevent frauds or errors. It is traditionally the case of the accountability to order product and the accountability to validate the invoice of the product order. In order to emend such business defects, a dissemination of responsibility components among multiple responsibilities has to be done.

- *Cardinality constraints*. The responsibility graph needs also to be checked at this step for alignment with cardinality requirement. E.g.: the number of accountabilities handled by a same responsibility is sometimes limited in order to avoid an unjustified increasing working. This constraint is to be balanced according to the work effort necessary for achieving each accountability.

3.5 STEP 5 Policy elicitation

This last step of our methodology aims at derogating policies from the responsibility model.

STEP 5 input: Input of step 5 is the process graphical representation issued from step 4.

STEP 5 output: Output of step 5 is a set of context dependant policies.

STEP 5 actions: The activity of that step aims at translating the responsibility graph in given policy format.

Sub-task 1: Each responsibility is assigned to an organisational role (such as Project Manager). In other words, capabilities and accountabilities of each responsibility are allocated to the roles. Different checks have to be done on this first instantiated model, in order to detect inconsistencies. Compliance to rules, checked during the previous step is again tested. For example, separation of duties (a responsibility can be protected against abuse of power, but the combination of two responsibilities for the same role may enable abuse) or cardinality constraints (individually a load of work for a responsibility can be supportable, but the

combination of many responsibilities may become insufferable. This check may include not only the current process level but also the organisational level).

Sub-task 2: Combining the role instantiated diagram and a set of roles allocated to organisation stakeholders, the diagram is instantiated to stakeholders, in which capabilities and accountabilities of responsibilities are allocated to stakeholders. Again, checks have to be done, in order to detect inconsistencies at this step (in the case of stakeholder having different process involved roles).

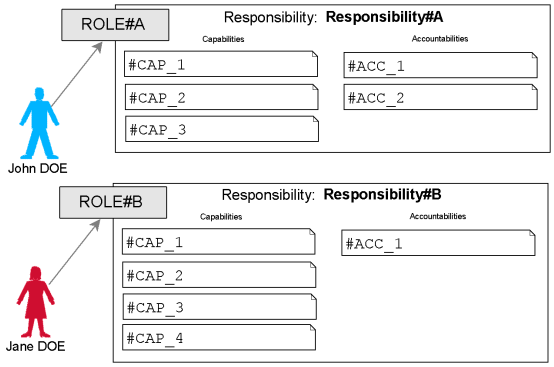

Fig. 10 Responsibilities instantiation

Sub-task 3: At this step, the diagram includes all minimum rights required by all the involved stakeholders for achieving process (by achieving all accountabilities). Using this responsibilities distribution, IT policies can be inferred using capabilities as authorizations, and accountabilities as obligations. A possible representation of these policies, described in [18], is the declarative control policy language XACML. Afterwards, the policy is deployed on the IT resources via a multi-agent system.

IV. Conclusions and Future Works

In the current economic context, improving ICT governance is an important matter. We propose in this paper to improve that field by introducing our formalization of the responsibility in an innovative responsibility model. This model is valuable when it is linked to another existing organizational model like Cobit or Cimosa and brings to that organizational model more guarantees regarding corporate governance requirements. The paper proposes also a methodology allowing defining, structure and managing the organization's responsibilities. To enhance and validate our work, we have deployed the methodology using the "Customer Complaints" process of Telindus Luxembourg SA. The case study lead on the one hand to potential improvements of the customer complaint process, while, on the other hand, it allowed to validate the methodology, but also to identify interesting ways of improving and extending it in future research.

Future works, based on the conclusion of the case study, will consist on improving the methodology with the addition of a global iterative refining layer. This layer aims at refining the responsibility models of the same domain together.

V. Acknowledgement

The results presented in this paper are a contribution from the SIM (Secure Identity Management) project and the RED (Reaction After Detection) project [19].

VI. References

[1] P. S.Sarbanes and M. Oxley, "Sarbanes-Oxley Act of 2002", 2002.
[2] Bank for International Settlements BIS: International Convergence of Capital Measurement and Capital Standards: Revised Framework – Comprehensive Version, 2006.
[3] European Union: Directive 95/46/EC of the European Parliament and of the Council. Official Journal of the European Communities, pp. 28-31, 1995.
[4] ISO/IEC 15504, "Information Technology – Process assessment", (parts 1-5), 2003-2006
[5] Christophe Feltus, André Rifaut, An Ontology for Requirements Analysis of Managers' Policies in Financial Institutions, I-ESA2007, Madeira, Portugal.
[6] André Rifaut, Christophe Feltus, Improving Operational Risk Management Systems by Formalizing the Basel II Regulation with Goal Models and the ISO/IEC 15504 Approach, REMO2V'2006, Luxembourg
[7] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R.Kuhn and R. Chandramouli, Proposed NIST Standard for Role-Based Access Control, ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001, Pages 224-274.
[8] R. Sandhu, J. Park, Usage Control: A Vision for Next Generation Access Control, The Second International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security, 2003.
[9] Abou El Kalam, A., El Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miège, A., Saurel, C., Trouessin, G. (2003), Organization-Based Access Control, IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy'03), 4-6 juin 2003, Côme, Italie, pp 120-131
[10] Control Objectives for Information and Related Technology (COBIT), Information Systems Audit and Control Association, http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981
[11] U.K. Office of Government Commerce, "A Code of Practice for IT Service Management," in Service Support, ITIL Managing Services, Stationery Office, London, United Kingdom (2005), Section 7.8, http://www.tsoshop.co.uk/bookstore.asp?FO=1159966&Action=Book&ProductID=0113300158.
[12] Bertino, E., Mileo, A., and Provetti, A. 2005. PDL with Preferences. IEEE international Workshop on Policies For Distributed Systems and Networks, Policy 2005 – Vol. 00, IEEE Computer Society, Washington, DC, 213-222.
[13] Yu, E. S. and Liu, L. 2001. Modelling Trust for System Design Using the i* Strategic Actors Framework. Workshop on Deception, Fraud, and Trust in Agent Societies Held During the Autonomous, Eds. Lecture Notes In Computer Science, vol. 2246. Springer-Verlag, London, 175-194.
[14] A. Antón, Goal-Based Requirements Analysi,. Second ICRE'96, Colorado Springs, USA, 1996.
[15] Robert Crook, Darrel Ince, Bashar Nuseibeh, Towards an Analytical Role Modelling Framework for Security Requirements, Security Requirements Group, Departement of Computing, The Open University, Walton Hall, Milton Keynes, MK7 6AA, UK.
[16] Vernadat F. B., Enterprise Modelling and Integration, Chapman & Hall, London (1995), ISBN 0-412-60550-3
[17] Togaf (2007), The Open Group Architecture Framework (TOGAF 8.1.1 'The Book'), 2007 Edition , Van Haren Publishing.
[18] Gateau, B., Feltus, C., Aubert J., Incoul, C. (2008), An Agent-based Framework for Identity Management: The Unsuspected Relation with ISO/IEC 15504, RCIS 2008, Morocco.
[19] http://projects.celtic-initiative.org/red/?Dissemination:Publications

Manuscript received September 30, 2008. Corresponding author: C. Feltus (e-mail: christophe.feltus@tudor.lu)